EXHIBIT 2

[redacted]

From: DigiCert <updates@digicert.com>
Sent: Monday, July 29, 2024 6:41 PM
To: Dmitry Manilov <Dmitry.Manilov@alegeus.com>
Subject: [Urgent Action Required] Reissue your certificates before 19:30 UTC on JULY 30, 2024.

If you are having trouble reading this email, read the online version [app.updates.digicert.com].

ACTION REQUIRED

Hello,

We're writing to inform you that DigiCert must revoke your certificates, no later than JULY 30, 2024, at 19:30 UTC.

To avoid disruption, you must reissue/rekey and reinstall the impacted certificates before they are revoked no later than JULY 30, 2024, at 19:30 UTC.

Why are we revoking your certificates?

DigiCert will be revoking certificates that did not have proper Domain Control Verification (DCV). Before issuing a certificate to a customer, DigiCert validates the customer's control or ownership over the domain name for which they are requesting a certificate using one of several methods approved by the CA/Browser Forum (CABF). One of these methods relies on the customer adding a DNS CNAME record which includes a random value provided to them by DigiCert. DigiCert then does a DNS lookup for the domain and verifies the same random value, thereby proving domain control by the customer.

There are multiple valid ways to add a DNS CNAME record with the random value provided for this purpose. One of them requires the random value to be prefixed with an underscore character. The underscore prefix ensures that the random value cannot collide with an actual

domain name that uses the same random value. While the odds of that happening are practically negligible, the validation is still deemed as non-compliant if it does not include the underscore prefix.

Recently, we learned that we did not include the underscore prefix with the random value used in some CNAME-based validation cases. This impacted approximately 0.4% of the domain validations we have in effect. Under strict CABF rules, certificates with an issue in their domain validation must be revoked within 24 hours, without exception.

For more detailed information regarding this incident, please visit: https://www.digicert.com/support/certificate-revocation-incident [app.updates.digicert.com]

What do you need to do?

To avoid disruption, you must reissue/rekey and reinstall the impacted certificates before they are revoked no later than JULY 30, 2024, at 19:30 UTC.

If you do not have access to a DigiCert account, please reach out to your partner to replace impacted certificates.

Instructions:

1. Login to your CertCentral [app.updates.digicert.com] account and view the CNAME Revocation Incident banner when you first login to see impacted certificates.
2. Go to the **Certificates > Orders** page and locate your impacted certificates.
3. Generate a new Certificate Signing Request (CSR) [app.updates.digicert.com].
4. On each certificate's **Order #** details page, in the **Certificate actions** dropdown, select **Reissue certificate**.
5. Complete any additional required validation steps [app.updates.digicert.com].
6. Install your reissued SSL/ TLS certificate [app.updates.digicert.com].

If you use a certificate management solution such as Trust Lifecycle Manager [app.updates.digicert.com], please refer to its instructions on how to automate replacement of impacted certificates.

For any questions, please contact your account manager or reach out to DigiCert Support using the information provided in your CertCentral account. If you are an end user of one of DigiCert's preferred Partners and do not have access to a DigiCert account, please contact your partner to replace certificates.

Sincerely,

The DigiCert Team